UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/648,211	08/25/2000	John S. Flowers	HVWD-01001US0-MEM/SBS	5311

758 7590 07/15/2005

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/648,211	FLOWERS ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34 and 36-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *44* is/are allowed.

6)☒ Claim(s) *1-28,30-34,36-43 and 45* is/are rejected.

7)☒ Claim(s) *29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 2 May 2005.

2. Claims 1-34 and 36-45 are pending in the application.

3. Claims 1-28, 30-34, 36-43 and 45 have been rejected.

4. Claim 44 has been allowed.

5. Claim 29 has been objected to for being dependent upon a rejected claim.

6. Claim 35 has been cancelled.

Response to Arguments

7. Applicant's arguments with respect to claims 1-28, 30-34, 36-43 and 45 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5, 8-20, 23-28, 30, 33, 34 and 39-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Zagorski et al U.S. Patent No. 6,789,216 B2.

As to claims 1, 13 and 39, Zagorski et al discloses a method of examining a network, including:

identifying an operating system of a remote host based on communications with the remote host through the network, including identifying a version and a patch level of the operating system [column 9 line 41 to column 10 line 46];

identifying a service of the remote host based on communications with the remote host through the network, including identifying a version and a patch level of the service [column 9 line 41 to column 10 line 46];

identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service [column 9 line 41 to column 10 line 46].

As to claims 2, 12, 17 and 45, Zagorski et al discloses that the step of identifying an operating system includes sending a first set of packets to the remote host and receiving a second set of packets from the remote host in response to the first set of packets [column 9 line 41 to column 10 line 46]. Zagorski et al discloses analyzing the second set of packets for inferential information indicative of the operating system. Zagorski et al discloses that the step of identifying a service includes sending a third set of packets to the remote host and receiving a fourth set of packets from the remote host in response to the third set of packets [column 9 line 41 to column 10 line 46]. Zagorski et al discloses that the information contained in the third set of packets is based on information received in the second set of packets. Zagorski et al discloses analyzing the fourth set of packets for inferential information indicative of the service [column 9 line 41 to column 10 line 46]. Zagorski et al discloses that the step of identifying a vulnerability includes comparing information contained in the second set of packets and the fourth set of

packets to preexisting vulnerability information in a database [column 9 line 41 to column 10 line 46].

As to claim 3, Zagorski et al suggests that the step of identifying an operating system includes sending three sets of packets to the remote host and receiving three respective sets of responsive packets from the remote host [column 9 line 41 to column 10 line 46].

As to claim 4, Zagorski et al discloses a method of examining a network, including:

nonintrusively identifying an operating system of a remote host including identifying a version of the operating system based on inferential information received from the remote host [column 9 line 41 to column 10 line 46];

nonintrusively identifying a service of the remote host including identifying a version of the service based on inferential information received from the remote host [column 9 line 41 to column 10 line 46].

As to claim 5, Zagorski et al discloses identifying a vulnerability of the network, as discussed above.

As to claim 8, Zagorski et al discloses identifying security policy violations on the network [column 11, lines 37-60].

As to claim 9, Zagorski et al discloses the step of identifying an operating system further includes identifying a patch level of the operating system. Zagorski et al discloses the step of identifying a service further includes identifying a patch level of the service, as discussed above.

As to claim 10, Zagorski et al discloses sending a selected packet to the remote host. Zagorski et al discloses receiving from the remote host a reflexive responsive packet [column 6 line 53 to column 7 line 5].

As to claim 11, Zagorski et al discloses sending a plurality of selected packets to the remote host. Zagorski et al discloses receiving from the remote host a plurality of reflexive responsive packets [column 7 line 49 to column 8 line 4].

As to claim 14, Zagorski et al discloses that the step of identifying a vulnerability includes using information obtained from the steps of identifying an operating system and identifying a service to identify the vulnerability, as discussed above.

As to claim 15, Zagorski et al discloses that the step of identifying an operating system further includes identifying a patch level of the operating system, as discussed above. Zagorski et al discloses that the step of identifying a service includes identifying a patch level of the service, as discussed above.

As to claim 16, Zagorski et al discloses sending a selected packet to the remote host. Zagorski et al discloses receiving from the remote host a reflexive responsive packet, as discussed above.

As to claim 18, Zagorski et al suggests that the information contained in the third set of packets is based on information received in the second set of packets. Zagorski et al suggests that the information contained in the fifth set of packets is based on information received in the fourth set of packets [column 7, lines 37-65].

As to claim 19, Zagorski et al discloses a method of examining a network, including:

sending a set of selected packets to a remote host on the network [column 9 line 41 to column 10 line 46];

receiving from the remote host a set of reflexive responsive packets [column 9 line 41 to column 10 line 46];

identifying conditions of the remote host by using inferential information received in the reflexive responsive packets, wherein the conditions include an operating system of the host, and a service of the host [column 9 line 41 to column 10 line 46].

As to claim 20, Zagorski et al discloses that the conditions further include a vulnerability of the host, as discussed above.

As to claim 23, Zagorski et al discloses that identifying an operating system includes identifying a version, as discussed above. Zagorski et al discloses that identifying a service includes identifying a version, as discussed above.

As to claim 24, Zagorski et al discloses that identifying an operating system includes identifying a version and a patch level, as discussed above. Zagorski et al discloses that identifying a service includes identifying a version and a patch level, as discussed above.

As to claim 25, Zagorski et al discloses that the step of sending a set of selected packets to a host on the network includes sending a plurality of sets of packets to the host. Zagorski et al discloses that the step of receiving from the remote host a set of reflexive responsive packets includes receiving a like plurality of sets of reflexive responsive packets [column 9 line 41 to column 10 line 46].

As to claims 26, 40 and 41, Zagorski et al discloses a method of detecting a vulnerability of a network, comprising:

sending a first set of test packets to a remote host on the network, as discussed above;

receiving a first set of reflexive packets from the remote host in response to the first set of test packets, as discussed above;

sending a second set of test packets to the remote host on the network, wherein information contained in the first set of test packets is based on inferential information contained in the first set of reflexive packets, as discussed above;

receiving a second set of reflexive packets from the remote host in response to the second set of test packets, as discussed above;

based on inferential information contained in the first set of reflexive packets, identifying an operating system of the remote host, including a version and a patch level , as discussed above; and

based on inferential information contained in the second set of reflexive packets, identifying a service of the remote host, including a version and a patch level , as discussed above.

As to claim 27, Zagorski et al discloses sending a seventh set of selected packets to a host on the network. Zagorski et al discloses receiving an eighth set of packets from the remote host in response to the seventh set of packets. Zagorski et al discloses sending a ninth set of selected packets to a host on the network. Zagorski et al discloses receiving a tenth set of packets from the remote host in response to the ninth set of packets. Zagorski et al discloses that based on information contained in the eight and tenth sets of packets, identifying a service of a host on the network, including a version and a patch level [column 9 line 41 to column 10 line 46].

As to claim 28, Zagorski et al discloses that based on information contained in at least the tenth sequence, identifying a vulnerability [column 6, lines 49-65].

As to claim 30, Zagorski et al discloses a method of examining a network, comprising:

sending a plurality of packets to a host on the network, as discussed above;

receiving a responsive plurality of packets from the host, as discussed above;

comparing inferential information in the responsive packets to information stored in a database;

based on the comparison, identifying a plurality of network conditions, including a vulnerability of the network [column 6, lines 49-65].

As to claim 33, Zagorski et al discloses a method of examining a network, comprising:

sending packets to a host on the network, as discussed above;

receiving a responsive packets from the host, as discussed above;

comparing inferential information in the responsive packets to information stored in a database, as discussed above; and

based on the comparison, inferring an unknown vulnerability [column 6, lines 49-65].

As to claim 34, Zagorski et al discloses a method of examining a network, comprising:

sending packets to a host on the network, as discussed above;

receiving responsive packets from the host, as discussed above;

comparing inferential information in the responsive packets to information stored in a database, as discussed above; and

based on the comparison, identifying a security policy violation [column 6, lines 49-65].

As to claim 42, Zagorski et al discloses receiving a set of selected packets from remote equipment, as discussed above. Zagorski et al discloses automatically sending a second set of packets to the remote equipment, which packets include information that enables the remote equipment to identify a vulnerability on the network, as discussed above

As to claim 43, Zagorski et al discloses a method for use by a host on a network, comprising:

receiving a first set of test packets from remote equipment, as discussed above;

automatically sending a first set of reflexive packets to the remote equipment, the first set of reflexive packets containing information generated according to a Request for Comment (RFC) protocol and indicative of an operating system, including a version and patch level [column 9 line 41 to column 10 line 46];

receiving a first test packet from the remote equipment as discussed above;

automatically sending a second set of reflexive packets to the remote equipment, the second set of reflexive packets containing information generated according to a Request For Comment (RFC) protocol and indicative of a service, including a version and patch level [column 9 line 41 to column 10 line 46];

wherein the first set of reflexive packets includes information that enables the remote equipment to identify the operating system on the host information that enables the remote equipment: to identify a service, including a version and a patch level [column 9 line 41 to column 10 line 46];

wherein the second set of reflexive packets includes information that enables the remote equipment to identify the service on the host, including a version and a patch level [column 9 line 41 to column 10 line 46].

9. Claims 31, 36 and 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Arnold et al U.S. Patent No. 5,440,723.

As to claim 31, Arnold et al discloses a method of examining a network, comprising:

sending packets to a host on the network [column 4 line 61 to column 5 line 16];

receiving responsive packets from the host [column 4 line 61 to column 5 line 16];

comparing inferential information in the responsive packets to information stored in a database [column 4 line 61 to column 5 line 16]; and

based on the comparison, identifying a Trojan application on the network [column 4 line 61 to column 5 line 16].

As to claim 36, Arnold et al discloses a system for examining a network, comprising:

database including a set of reflex signatures [column 5, lines 29-46];

a packet generator [column 5, lines 29-46];

a comparison unit in communication with the packet generator and the database [column 7, lines 11-33];

wherein the packet generator is designed to generate and transmit a plurality of test packets to the network [column 7, lines 11-33];

wherein the comparison unit is designed to receive responsive packets from the network and to compare inferential information from the reflex signatures [column 7, lines 11-33].

the comparison unit is further designed to identify a vulnerability in the network based on its comparison of packet information with reflex signatures [column 4 line 61 to column 5 line 16].

As to claim 38, Arnold et al discloses that the comparison unit is designed to provide information to the packet generator, and wherein the packet generator is designed to use the information to selectively generate packets [column 5, lines 29-46].

10. Claim 32 is rejected under 35 U.S.C. 102(e) as being anticipated by Diersch et al U.S. Patent No. 6,101,606.

As to claim 32, Diersch et al discloses a method of examining a network, comprising:

sending packets to a host on the network [column 5, lines 11-65];

receiving responsive packets from the host [column 5, lines 11-65];

comparing inferential information in the responsive packets to information stored in a database [column 5, lines 11-65]; and

based on the comparison, identifying unauthorized software use on the network [column 5, lines 11-65].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 6 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zagorski et al U.S. Patent No. 6,789,216 B2 as applied to claim 1 above, and further in view of Drake U.S. Patent No. 6,006,328.

As to claims 6 and 22, Zagorski et al does not teach identifying a Trojan application on the host.

Drake teaches identifying a Trojan application on the host [column 1 line 56 to column 2 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zagorski et al so that when the operating system is being identified that a Trojan application on the host was also identified.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zagorski et al by the teaching of Drake because it prevents eavesdropping, prevents disassembly and examination, detects tampering, prevents execution-tracing and ensures authenticity [column 5, lines 3-14].

12. Claims 7 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zagorski et al U.S. Patent No. 6,789,216 B2 as applied to claim 1 above, and further in view of Hornbuckle U.S. Patent No. 5,388,211.

As to claims 7 and 21, Zagorski et al does not teach identifying unauthorized software use on the host.

Hornbuckle teaches identifying unauthorized software use on the host [column 3, lines 6-63].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zagorski et al so that when the operating system is being identified that unauthorized software use was also identified on the host.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zagorski et al by the teaching of Hornbuckle because it prevents theft, copying, vandalism or modification [column 3, lines 6-15].

13. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al U.S. Patent No. 5,440,723 as applied to claim 35 above, and further in view of Zagorski et al U.S. Patent No. 6,789,216 B2.

As to claim 37, Arnold et al does not teach that the comparison unit is further designed to identify an operating system type, version, and patch level and a service type, version, and patch level of a host on the network.

Zagorski et al teaches a comparison unit that is designed to identify an operating system type, version, and patch level and a service type, version, and patch level of a host on the network, as discussed above.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Arnold et al so that the comparison unit would have identified an operating system type, version, and patch level and a service type, version, and patch level of a host on the network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Arnold et al by the teaching of Zagorski et al because the examiner asserts that certain versions of some operating system are known to have known vulnerabilities as well as service types and patch levels. Therefore, it would be necessary to check these elements on a host to prevent exploitations on these known vulnerabilities.

Claim Objections

14. Claim 29 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As to claim 29, prior art des not teach a first set of packets that includes: a SYN Packet with false flag in the TCP option header; a Fragmented UDP packet with malformed header (any header inconsistency is sufficient), where the packet is 8K in size; a FIN Packets of a selected variable size or a FIN packet without the ACK or SYN flag properly set; and a generic, well-formed ICMP ECHO request packet. Prior art does not teach a third set of packets includes: a generic well-formed TCP Header set to 1024 bytes in size; a packet requesting an ICMP Timestamp; a packet with min/max segment size set to a selected variable value; and a UDP packet with the fragment bit set. Prior art does not teach a fifth set of packets includes: a TCP Packet with the header and options set incorrectly; a well-formed ICN11P Packet; a

Fragmented TCP or UDP packet; a packet with an empty TCP window or a window set to zero; a generic TCP Packet with 8K of random data; and a SYN Packet with ACK and RST flags set.

Allowable Subject Matter

15. Claim 44 is allowed.

As to claim 44, prior art does not disclose or fairly suggest that the first set of packets comprises an operating system packet to determine the operating system. Prior art does not disclose or fairly suggest an operating system version packet to determine the operating system version based on the determined operating system. Prior art does not disclose or fairly suggest an operating system patch level packet to determine the operating system patch level based on the determined operating system version. Prior art does not disclose or fairly suggest identifying a service of the remote host that includes a version and a patch level of the service with a second set of packets based on at least one of the first set off packets. Prior art does not disclose or fairly suggest that the first set of packets comprising a service packet to determine the service. Prior art does not disclose or fairly suggest service version packet to determine the service version based on the determined service. Prior art does not disclose or fairly suggest a service patch level packet to determine the service patch level based on the determined service version. Prior art does not disclose or fairly suggest identifying a vulnerability of the network based on information obtained from the steps of identifying an operating system and identifying a service.

Conclusion

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
July 6, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100